

**VYSOKÁ ŠKOLA BÁŇSKÁ –
TECHNICKÁ UNIVERZITA OSTRAVA**

Hornicko-geologická fakulta
Institut ekonomiky a systému řízení

Ochrana osobních údajů

bakalářská práce

Autor:

Jiří Husák

Vedoucí bakalářské práce:

PhDr. Ing. Jan Gottfried

Most 2010

Anotace

Tato bakalářská práce je zaměřená na právní úpravu ochrany osobních údajů v právním řádu České republiky a na právní normy Evropské unie. V bakalářské práci jsou definovány základní pojmy ochrany osobních údajů z hlediska práva. Dále se tato práce zaměřuje na stále větší rozšiřování systému RFID (Radio Frequency Identification) a na jeho možnosti automaticky zpracovávat údaje a s tím související problematika úpravy stávajících norem ochrany osobních údajů.

Klíčová slova

ochrana osobních údajů, RFID, osobní údaj, citlivý údaj,

Annotation

This bachelor's thesis is focused on the legal aspects of personal data protection in the legislation of the Czech Republic and the legal norms of the European Union. The thesis defines the basic notions of personal data protection in law. Furthermore, this work focuses on the increasing expansion of RFID (Radio Frequency Identification) and its ability to automatically process data and the related issue of adapting existing legal norms of personal data protection.

Keywords

personal data protection, RFID, personal data, sensitive data

Prohlášení

Místopřísežně prohlašuji, že jsem celou práci, vypracoval samostatně, pouze s použitím pramenů a literatury uvedených v seznamu použité literatury.

V Mostě, 30. 4. 2010

Jiří Husák

Obsah:

1. ÚVOD	1
2. VYMEZENÍ ZÁKLADNÍCH POJMŮ.....	2
2.1 OSOBNÍ ÚDAJ	2
2.2 CITLIVÉ OSOBNÍ ÚDAJE	3
2.3 ANONYMNÍ ÚDAJE	4
2.4 ZVEŘEJNĚNÉ OSOBNÍ ÚDAJE	4
2.5 SUBJEKTY PRÁVNÍ ÚPRAVY	5
2.5.1 Subjekt údajů	5
2.5.2 Správce.....	5
2.5.3 Zpracovatel.....	6
2.5.4 Příjemce.....	6
2.6 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	6
2.6.1 Shromažďování osobních údajů.....	7
2.6.2 Uchovávání osobních údajů	7
2.6.3 Blokování osobních údajů	7
2.6.4 Likvidace osobních údajů	7
2.7 DATOVÝ SOUBOR	7
2.8 OCHRANA OSOBNÍCH ÚDAJŮ	8
3. ZÁKONNÁ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ	9
3.1 ZÁKONNÁ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ Z POHLEDU NOREM ČESKÉ REPUBLIKY	9
3.1.1 Listina základních lidských práv a svobod	9
3.1.2 Zákon na ochranu osobních údajů č. 101/2000	10
3.1.3 Zákon o svobodném přístupu k informacím č. 106/1999 Sb.....	11
3.2 ZÁKONNÁ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ Z POHLEDU NOREM EU	11
3.2.1 Směrnice EP 95/46/ES.....	13
3.2.2 Nařízení 45/2001/ES	13
3.2.3 Doporučení komise 2009/387/ES ze dne 12. května 2009.....	13
4. DOPADY OCHRANY OSOBNÍCH ÚDAJŮ NA PROVOZOVATELE RFID ZAŘÍZENÍ	15
4.1 POJEM RFID A MOŽNOSTI VYUŽITÍ.....	15
4.2 POVINNOSTI PROVOZOVATELŮ RFID ZAŘÍZENÍ.....	16
4.3 DOPORUČENÍ PRO PROVOZOVATELE.....	19
5. DOPADY OCHRANY OSOBNÍCH ÚDAJŮ NA UŽIVATELE.....	21
5.1 MOŽNOSTI OCHRANY OSOBNÍCH ÚDAJŮ	21
5.2 PRÁVA PŘI OCHRANĚ OSOBNÍCH ÚDAJŮ	21
5.3 DOPORUČENÍ	22
6. ZÁVĚR.....	23

1. Úvod

Osobní údaje a jejich ochrana, na které je zaměřena tato bakalářská práce, jsou celospolečensky diskutovaným tématem. Toto téma se týká jak jednotlivců, tak celé společnosti. S každým z nás je od narození spojena informace, která ho jednoznačně identifikuje a provází ho celý život. Jedná se o jméno, příjmení, datum a místo narození, pohlaví a v neposlední řadě rodné číslo jako národní identifikátor osoby. Mezi další údaje patří také citlivé údaje, jako je třeba národnost nebo zdravotní stav. S těmito osobními údaji je zapotřebí zacházet s náležitou opatrností protože mohou vést k diskriminaci jedince.

Vzhledem k tomu, že žijeme v době, kdy dochází k nebývalému rozvoji a možnostem nových informačních a komunikačních technologií, rostou i možnosti jejich zneužití. Proto je důležité klást takový důraz na ochranu osobních údajů proti možnostem jejich zneužití. V dnešním světě informací má každá informace svoji cenu a tak se i z našich osobních a soukromých údajů může stát pouhé zboží.

Jednou z technologií, která začíná ovládat trh s informacemi je RFID (Radio Frequency Identification). Vzhledem k možnostem použití, které je schopna poskytnout bude zapotřebí informovat širokou veřejnost o těchto možnostech a zároveň jim zabezpečit jejich právo na soukromí.

Cílem této práce je přiblížit problematiku právní ochrany osobních údajů, definovat základní pojmy a seznámit s právními normami. První dvě kapitoly jsou věnovány vysvětlení pojmů a v jakých právních normách jsou ukotveny práva na ochranu osobních údajů. V dalších kapitolách se podíváme na dopady používání RFID technologie na provozovatele a na uživatele.

2. Vymezení základních pojmů

Pro lepší pochopení a vyjasnění pojmů o ochraně osobních údajů je důležité si definovat základní klíčové pojmy. Nejdůležitějším ze základních pojmů je „osobní údaj“. Nemůžeme ho ovšem zaměňovat s pojmem „projev osobní povahy“, který je formulován v § 11 Občanského zákoníku *„fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy“*¹. Jedná se o dva samostatné právní pojmy. Za určitých okolností u nich ovšem může docházet k jejich prolínání.

2.1 Osobní údaj

Zjednodušeně lze říci, že osobním údajem je prakticky cokoli, co se týká naší osoby, tedy údaj, na základě něhož je možné nás identifikovat a co s námi přímo souvisí. Definici tohoto pojmu z právního hlediska nalezneme přímo v zákoně č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších platných předpisů (dále jen „zákon o ochraně osobních údajů“), kde je v § 4 napsáno, že *„osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“*². Pokud lze podle této definice přímo ze shromážděných údajů, nebo na jejich základě jinak identifikovat fyzickou osobu, potom se jedná o osobní údaj. Přičemž znakem osobního údaje je, že jej nelze zaměnit s jiným subjektem údajů.

Z toho vyplývá, že osobním údajem je každý údaj, který je uvedený do vztahu k fyzické osobě. Nemůžeme tedy hovořit ani uvažovat o samotném osobním údaji. Osobní údaje existují jenom ve spojení se subjektem údajů. Kterákoliv osobní informace, která nebude ve spojení s jednoznačně určenou

¹ Zákon č. 40/1964 Sb., občanský zákoník

² Zákon č. 101/2000 Sb., o ochraně osobních údajů

osobou, anebo dle které nebude možné tuto osobu identifikovat, není osobním údajem.

Osobní údaje můžeme rozdělit a definovat na určité typy a to nejen z hlediska zákona. Údaje tedy dělíme do několika skupin.

- Údaje identifikační a kontaktní
- Popisné údaje obecné
- Popisné údaje transakční (generované správcem neboli provozní)
- Údaje jiného subjektu údajů

2.2 Citlivé osobní údaje

Pro citlivé údaje platí mnohem přísnější pravidla než pro ostatní osobní údaje a to především z hlediska jejich zneužitelnosti. Bývají také označovány jako senzitivní a pokud se s nimi nesprávně manipuluje, mohou mít pro subjekt údajů i závažné následky. Jsou v právních předpisech výslovně vyčleněny a je jim poskytována zvýšená ochrana. Citlivý osobní údaj je v zákoně o ochraně osobních údajů definován v §4 písm. b) *„pro účely tohoto zákona se rozumí citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“*³. Zpracování těchto údajů je možné provádět pouze za jasně stanovených podmínek s výslovným souhlasem k jejich zpracování, pokud zákon výslovně nestanoví jinak.

Ve směrnici EP č. 95/46/ES se citlivé údaje definují, jako zvláštní kategorie osobních údajů kde je uvedeno i vnitrostátní identifikační číslo nebo jakýkoliv jiný identifikátor obecného významu. V české republice je takovým údajem rodné číslo. Rodné číslo v sobě obsahuje dva osobní údaje a tím je datum narození a pohlaví subjektu údajů.

³ Ustanovení §4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů

Pokud se podíváme blíže na jednotlivé citlivé údaje tak zjistíme, že jejich nesprávné použití může mít pro subjekt údajů závažné důsledky.

2.3 Anonymní údaje

Anonymním údajem je dle zákona o ochraně osobních údajů takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů. Tyto údaje mohou vzniknout buď anonymizací anebo jsou shromážděny v původním tvaru. V případě anonymizace se nejčastěji bude jednat o databázový soubor, kde dojde k odstranění příjmení a jména, případně dalších znaků a přestane existovat reálná možnost propojit tyto informace zpět a tím určit subjekt údajů. V druhém případě se může jednat o průzkum trhu, kdy informace získáme od konkrétního subjektu údajů, avšak anonymně. U zpracování anonymních údajů platí, že je lze zpracovávat bez souhlasu subjektu údajů a nepodléhá režimu zákona o ochraně osobních údajů. Nejčastěji se s nimi setkáme v oblasti statistiky, výzkumu a marketingu.

2.4 Zveřejněné osobní údaje

Za zveřejněný osobní údaj v souladu se zákonem o ochraně osobních údajů považujeme osobní údaj zpřístupněný hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Pod pojmem hromadným sdělovacím prostředkem si můžeme představit periodický tisk, rozhlasové vysílání, televizní vysílání, internet a další.

Jiným veřejným sdělením může být například informace podaná v knize, na plakátě nebo v oblasti veřejné správy v souvislosti s veřejnou vyhláškou. Doručení veřejnou vyhláškou se řídí podmínkami a způsobem, které stanovuje správní řád⁴. Hodně diskutovanou otázkou byly informace z rady obce, jako je zápis z jednání zastupitelstva obce a zápis z jednání rady obce. V těchto dokumentech se často nachází osobní údaje o fyzických osobách, například při uzavírání smluv s obcí. Zde dochází ke kolizi několika zákonů, jako je zákon o svobodném přístupu

⁴ Ustanovení §25 zákona č. 500/2004 Sb., správní řád

k informacím, zákon o obcích a zákon o ochraně osobních údajů. Touto otázkou se zabýval i nejvyšší správní soud⁵.

2.5 Subjekty právní úpravy

Z hlediska vymezení pojmů se v zákoně o ochraně osobních údajů setkáváme s dalšími pojmy, které se přímo týkají fyzických osob, dále subjektů, které s údaji pracují a využívají – subjekt údajů, správce, zpracovatel a příjemce.

2.5.1 Subjekt údajů

Dle § 4 písm. k) zákona o ochraně osobních údajů je „*subjektem údajů fyzická osoba, k níž se osobní údaje vztahují*“⁶. Jedná se tedy o každou fyzickou osobu, které se osobní údaje týkají. Jedná se o všechny fyzické osoby na území české republiky, bez omezení věku, státní příslušnosti či způsobilosti k právním úkonům apod.

2.5.2 Správce

Dle § 4 písm. j) zákona o ochraně osobních údajů je „*správce každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracování osobních údajů může správce pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak*“⁶. Z výše uvedeného vyplývá, že správcem může být jak fyzická osoba, tak i právnická osoba, podnikatel i subjekt nepodnikající, orgán veřejné moci, nebo soukromý subjekt.⁷ Podstatné pro správce je, aby tento byl v souladu se zákonem o ochraně osobních údajů bez ohledu na jeho určení.

Správce je subjekt i tehdy pokud osobní údaje nezpracovává. Zpracováním může být zmocněn na základě zvláštního zákona nebo právně platné smlouvy zpracovatel. Tato smlouva musí obsahovat zejména informace v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá. Zpracovatel by měl

⁵ rozsudek Nejvyššího správního soudu ze dne 25. 8. 2005, čj. 6 As 40/2004 - 62, www.nssoud.cz

⁶ zákon č. 101/2000 Sb., o ochraně osobních údajů

⁷ <http://business.center.cz/business/pojmy/p498-spravce.aspx>

ve smlouvě poskytnout záruky o organizačním a technickém zabezpečení osobních údajů.

2.5.3 Zpracovatel

Dle § 4 písm. k) zákona o ochraně osobních údajů je „*zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona*“⁸. Zpracovatel neurčuje účel ani prostředky zpracování osobních údajů. Zpracovatel je též jakýkoliv subjekt, který provádí jakoukoliv činnost související se zpracováním.

2.5.4 Příjemce

Dle § 4 písm. o) zákona o ochraně osobních údajů je „*příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g)*“⁸. Za příjemce nejsou považovány subjekty, které zpracovávají osobní údaje při výkonu kontroly, dozoru, dohledu nebo regulace v souvislosti s výkonem veřejné moci⁹. Účelem je vymezit osoby, které nejsou správci ani zpracovateli, ale mohou přijít do styku s osobními údaji.

2.6 Zpracování osobních údajů

Pod pojmem zpracování osobních údajů si můžeme představit každou operaci nebo soubor operací, které správce nebo zpracovatel systematicky provádí s osobními údaji. Podle platné právní úpravy není rozhodné, zda dochází ke zpracování osobních dat automatizovaně nebo manuálně. Zpracováním se rozumí shromažďování údajů, ukládání na nosiče informací, zpřístupňování, ale též i operace jako je vyhledávání, třídění či blokování nebo likvidace dat. Zákon o ochraně osobních údajů uvádí výčet operací, které se za zpracování považují, a to shromažďování, uchovávání, blokování a likvidace osobních údajů.

⁸ zákon č. 101/2000 Sb., o ochraně osobních údajů

⁹ § 3 odst. 6 písm. g) zákona č. 101/2000 Sb., o ochraně osobních údajů

2.6.1 Shromažďování osobních údajů

Mělo by se jednat o cílený sběr osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.¹⁰ Stanovení cíle je hlavním znakem pro shromažďování osobních údajů a měl by být znám již při jejich získávání.

2.6.2 Uchovávání osobních údajů

Udržování osobních údajů v podobě, která umožňuje jejich další zpracování. Údaje musí být pro správce trvale dosažitelné za účelem jejich zpracování. Osobní údaje mohou být uchovávány pouze po dobu trvání účelu, pro jaký byla pořízena.

2.6.3 Blokování osobních údajů

Je takový stav osobního údaje, kdy je po určitou dobu nepřístupný a nelze jej ani jakkoliv zpracovávat a upravovat. Při blokování osobních údajů se tyto stávají nepřístupné pro správce, zpracovatele i jiné subjekty. Tento stav je stavem dočasným. Může se jednat o záměrné jednání správce nebo zpracovatele nebo se jedná o stav, kdy kontrolní orgán zakáže zpracování těchto údajů jako určitou formu opatření. Po pominutí důvodů pro blokování lze údaje opět zpracovávat.

2.6.4 Likvidace osobních údajů

Jde o úkon s osobními údaji, kdy dojde k jejich trvalému vyloučení ze zpracování, fyzickému zničení nosiče nebo fyzickému vymazání. K tomuto kroku může dojít, pokud pomine účel, pro který byly osobní údaje zpracovávány nebo také na žádost subjektu údajů k ochraně jeho práv.

2.7 Datový soubor

Datovým souborem se dle § 4 písm. m) zákona o ochraně osobních údajů rozumí „evidencí nebo datovým souborem osobních údajů (dále jen „datový

¹⁰ <http://business.center.cz/business/pojmy/p494-shromazdovani-osobnich-udaju.aspx>

soubor“) jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií“. Datovým souborem je jak lístková kartotéka, spis nebo registr ve kterých bývají třídícím prvkem například abecední pořádek, datum pořízení záznamu nebo místo pořízení. V současnosti se většina záznamů zpracovávána v elektronické podobě a jejich zpracování probíhá automatizovaně.

2.8 Ochrana osobních údajů

Prámem každého občana je zaručení ochrany osobních údajů, které je upraveno právními normami vydávanými výkonnou mocí státu. Při práci s nimi je třeba dodržovat určitá pravidla, jako je např. uvedeno v § 13 odst. (2) zákona na ochranu osobních údajů *„Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko - organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy“*¹¹. Vydání zákona na ochranu osobních údajů bylo reakcí na rozšíření již existujícího právního rámce ochrany, neboť vzhledem k prudkému nárůstu shromažďování osobních údajů již Listina základních práv a svobod nebyla dostačující.

¹¹ zákon č. 101/2000 Sb., o ochraně osobních údajů

3. Zákonná úprava ochrany osobních údajů

V dnešní době se zpracování osobních údajů stává čím dál více automatizovanější a s vývojem elektronických systémů i jednodušší. Z důvodu nutnosti tyto údaje chránit byly přijaty právní normy a ustanoveny orgány, které se ochranou osobních údajů zabývají.

Úplně prvním zákonem na ochranu osobních údajů je již zrušený zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Byly v něm poprvé definovány pojmy jako informace, zpracování informace, provozování informačního systému, likvidace informace apod. Stanovil také určitá práva a povinnosti pro nakládání s osobními údaji.

3.1 Zákonná úprava ochrany osobních údajů z pohledu norem České republiky

V současné době základními právními normami, ze kterých vychází ochrana osobních údajů v České republice, jsou zákon č. 2/1993 Sb., listina základních práv a svobod, ve znění pozdějších platných předpisů (dále jen „Listina základních práv a svobod“), zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších platných předpisů a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších platných předpisů.

3.1.1 Listina základních lidských práv a svobod

Ochrana osobních údajů je v České republice zařazena mezi základní lidská práva a je upravena Listinou základních práv a svobod, která je v souladu se zákonem č. 1/1993 Sb., ústava České republiky článkem 3 součástí ústavního pořádku České republiky¹². Dle hlavy druhé, oddílu prvního, listiny základních práv a svobod má každý právo na ochranu osobních údajů, zejména dle článku 10 a to:

Článek 10, bod (1) *„Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.“*

¹² Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Článek 10, bod (2) „Každý má právo na ochranu před neoprávněným zasahováním do soukromého a osobního života.“

Článek 10, bod (3) „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“

Z výše uvedeného vyplývá, že k problematice zpracování osobních údajů se vztahuje zejména odstavec 3 článku 10 Listiny základních práv a svobod. Ustanovení článku 10 Listiny základních práv a svobod je upraveno řadou právních norem, jedním z nich, který ochranu osobních údajů upravuje zejména z obecného hlediska, je zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších platných předpisů.

3.1.2 Zákon na ochranu osobních údajů č. 101/2000

Vzhledem k již nedostačující formulaci pojmu ochrana osobních údajů podle zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl aplikován především na informace obsažené v informačních systémech, došlo k vytvoření nové právní úpravy, jež z hlediska ochrany osobních údajů byla obecnější a aplikovatelná na jakýkoliv sběr, zpracování a uchování osobních údajů. Také bylo potřeba sjednocení z evropskou legislativou podle směrnice EP 95/46/ES ze dne 24. října 1995.

Zákon o ochraně osobních údajů je především obecnou právní úpravou, jsou v něm definovány odchylky, které jsou upraveny dalšími zvláštními zákony, jejichž ustanovení mají přednost před obecnou právní normou. Zvláštními zákony, na které zákon o ochraně osobních údajů odkazuje, jsou např.:

- zákon č. 238/1991 Sb., o Policii České republiky, ve znění pozdějších platných předpisů
- zákon č. 21/1992 Sb., o bankách, ve znění pozdějších platných předpisů
- zákon č.13/1993 Sb., celní zákon, ve znění pozdějších platných předpisů
- zákon č.328/1999 Sb., o občanských průkazech, ve znění pozdějších platných předpisů
- zákon č. 301/2000 Sb., o matrikách, jménu a příjmení, ve znění pozdějších platných předpisů

- zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činnostmi bývalé Státní bezpečnosti, ve znění pozdějších platných předpisů
- zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů

Všechny zvláštní právní úpravy, na které zákon o ochraně osobních údajů odkazuje, musí tuto obecnou právní úpravu respektovat.

3.1.3 Zákon o svobodném přístupu k informacím č. 106/1999 Sb.

Dle hlavy druhé, oddílu druhého Listiny základních práv a svobod, článku 17, odst. (1) „*Svoboda projevu a právo na informace jsou zaručeny.*“¹³ V civilizovaném světě je možnost přístupu k informacím brána jako určitý stupeň míry demokracie. Svoboda projevu a právo na informace dle Listiny základních práv a svobod jsou dále upraveny zákonem č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších platných předpisů¹⁴. Dle tohoto zákona mají občané a jiné fyzické a právnické osoby právo na to, být dostatečně informovány. Zároveň mají dotčené osoby v souladu se zákonem na ochranu osobních údajů právo na ochranu osobních údajů, čímž dochází k určitému právnímu střetu. Z ucelenějšího pohledu se však zákon na ochranu osobních údajů a zákon o svobodném přístupu k informacím doplňují.

3.2 Zákonná úprava ochrany osobních údajů z pohledu norem EU

Po vstupu České republiky do Evropské unie dochází k integraci evropských norem a doporučení do českých právních norem. Z hlediska EU se ochraně osobních údajů věnují především tyto právní normy¹⁵:

- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat - pro ČR s účinností od 1. listopadu 2001

¹³ zákon č. 2/1993 Sb., listina základních práv a svobod

¹⁴ zákon č. 106/1999 Sb., o svobodném přístupu k informacím

¹⁵ <http://www.uoou.cz/uoou.aspx?menu=4&submenu=6>

- Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat – pro ČR s účinností od 1. července 2004
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací – tato směrnice byla změněna Směrnicí Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, a také Směrnicí Evropského parlamentu a rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.
- Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008, o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech
- Doporučení Komise 2009/387/ES ze dne 12. května 2009, o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence

Pohyb osobních údajů a jeho zpracování vychází zejména ze Směrnice EP 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Pozornost je také vhodné věnovat doporučení

Komise 2009/387/ES o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence ze dne 12. 5. 2009.

3.2.1 Směrnice EP 95/46/ES

Tato směrnice ochrání fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů byla přijata na podporu jednotného trhu kvůli rozdílu v národních legislativách členských států, které bránily volnému pohybu osobních údajů mezi členskými státy. Směrnice má rozsáhlý záběr a vztahuje se na „všechny operace nebo soubor operací, které se týkají osobních údajů“ (tzn. zpracování), včetně jejich shromažďování, ukládání a zpřístupňování¹⁶.

3.2.2 Nařízení 45/2001/ES

Cílem tohoto nařízení je zajistit nejen účinné dodržování předpisů na ochranu základních lidských práv a svobod fyzických osob, ale zajistit i volný pohyb osobních údajů mezi členskými státy a orgány a institucemi Společenství.

Nařízení definuje zásady pro práci s údaji, práva subjektu údajů a bezpečnost zpracování. V každém orgánu a instituci zřizuje inspektora pro dohled nad osobními údaji.

Dále na základě tohoto nařízení vznikl nezávislý orgán dozoru nad zpracováním osobních údajů v institucích a orgánech EU – Evropský inspektor ochrany osobních údajů.

3.2.3 Doporučení komise 2009/387/ES ze dne 12. května 2009

o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence. Jedná se o doporučení pro členské státy, které si vyžádalo stále rozšířenější používání technologie RFID.

Jsou zde nově definované pojmy jako identifikace na základě rádiové frekvence, etiketa RFID, čtecí nebo zapisovací zařízení RFID, aplikace RFID,

¹⁶ <http://www.ikaros.cz/node/4552#6>

provozovatel RFID, bezpečnostní informace a sledování. Posledně jmenovaný pojem je z nich asi nejdůležitější protože nám jasně definuje, co se rozumí pojmem sledování. Je to „jakákoliv činnost vykonávaná za účelem zjištění, pozorování, reprodukování nebo zaznamenání údajů o místě, na němž se jednotlivec nachází, jeho pohybu, činnosti nebo stavu¹⁷“.

Všechny státy Evropského společenství by měly v souladu s tímto doporučením přijmout závazná opatření a upozornit všechny strany, které se podílejí na navrhování a provozování aplikací RFID v EU.

¹⁷ Doporučení komise 2009/387/ES ze dne 12. května 2009 bod 3. písm. g

4. Dopady ochrany osobních údajů na provozovatele RFID zařízení

4.1 Pojem RFID a možnosti využití

Současný pokrok techniky a technologií nám stále častěji přináší do života nové možnosti automatické identifikace a sběru údajů pomocí RFID. Pod pojmem RFID (Radio-frequency identification) se skrývá moderní bezkontaktní systém identifikace založený na radiové frekvenci. Prostřednictvím paměťových čipů dovolu je přiřazení jednoznačného identifikátoru anebo jiných informací k jakémukoliv subjektu.

Okruh využití této technologie je velice široký a můžeme se s ní setkat například v logistice, výrobě, evidenci majetku, zdravotnictví a dalších aplikacích. Základní myšlenkou RFID je identifikace objektu na větší vzdálenosti, bez přímé viditelnosti a s možností zpracování více objektů současně. Díky tomu dochází k zefektivnění a urychlení procesů. Na základě těchto výhod se použití čipové technologie jeví jako náhrada za čárové kódy, jejichž omezení jsou daná podmínkami čtení těchto kódů.

Více používaný pasivní RFID čip vysílá číslo (EPC – Electronic product key), které je určeno při výrobě nebo obsahuje paměť, ze které lze číst a zapisovat informace. K odeslání těchto informací je zapotřebí snímač, který vysílá do okolí impulsy. Čip, který je v blízkosti tohoto vysílače, využije vysílaného impulsu ke svému nabití a snímači odešle své informace. Vzdálenost, od které je možno číst informace je u pasivních čipů od 0,5m až do 10m.

Složitější a dražší aktivní RFID čip vysílá údaje do okolí sám. To mu umožňuje vlastní baterie, která vydrží po dobu až 5 let. Čip má na rozdíl od pasivního RFID větší velikost paměti, a to až 100Kb a větší vzdálenost na čtení až 100m. Protože obsahují baterii, jsou méně odolné vůči teplotám a je nutné provádět po určité době její výměnu.

RFID může urychlovat proces příjmu, výdaje, přesunu a inventarizace produktů, odstraňuje chyby obsluhy a má velkou odolnost vůči poškození kromě

elektromagnetického. Dají se implementovat do výrobků nebo obalů přímo ve výrobě. Nevýhodou jsou náklady na investici do nového systému. Je zapotřebí nákup nové technologie jako čtecí zařízení, změna procesů, úpravy software a školení obsluhy. Částečně tyto náklady kompenzují výhody, jako jsou úspory v nákladech na obsluhu, rychlost procesu, efektivní plánování skladového hospodářství apod.

U nás patří mezi mediálně známější projekty použití RFID technologie například čipová karta českých drah In-karta, čipová karta hlavního města Praha nazvaná Opencard, výběr mýtného na dálnicích a zpoplatněných komunikacích. Další možností využití je autorizace při vstupu do objektu. Často bývají propojeny s kamerovým systémem. U takto využívaných systémů vzniká dost často problém, že se shromažďuje a uchovává více dat, než je třeba potřeba. Například čas vstupu a odchodu, frekvence navštěvování objektu s následnou možností identifikace kamerovým systémem aj.

Způsobů využití RFID technologie je opravdu mnoho a není pravděpodobně oblast nebo obor lidské činnosti, kde by nenašel uplatnění.

4.2 Povinnosti provozovatelů RFID zařízení

Jedním z prvních dokumentů zabývajících se problematikou RFID technologií a ochrany osobních údajů na evropské úrovni byl dokument pracovní skupiny pro ochranu fyzických osob podle článku 29 směrnice 95/46/ES (WP29)¹⁸. Na základě jednání s výrobcí, uživateli, obhájci soukromí a dalšími zainteresovanými stranami vznikl dokument WP 105¹⁹, který měl za cíl poskytnout výrobcům i orgánům pro normalizaci RFID pokyny pro vytvoření takové technologie, která bude respektovat soukromí a na straně druhé poskytnout uživatelům RFID návod k používání základních zásad stanovených ve směrnici Evropského společenství.

Všichni správci údajů, kteří shromažďují údaje v rámci využívání RFID, musejí dodržovat všeobecné zásady ochrany údajů podle směrnice 95/46ES, včetně:

¹⁸ Směrnice 95/46/ES článek (29)

¹⁹ Dokument WP 105 [on-line] http://www.uoou.cz/files/zahr_EK_WP29_105.pdf

Používat zásadu omezení účelu

Tato zásada zakazuje další zpracování, které je neslučitelné s účely shromažďování.

Zásada kvality údajů

Tato zásada vyžaduje, aby osobní údaje byly podstatné a v množství úměrném účelům, pro které jsou shromažďovány. Proto se nesmějí shromažďovat žádné nepodstatné údaje, a jestliže již byly shromážděny, musejí být vymazány. Vyžaduje se také, aby údaje byly přesné a aktuální.

Zásada uchovávání

Tato zásada vyžaduje, aby osobní údaje nebyly uchovávány déle, než je nezbytné pro účel, pro který byly údaje shromážděny nebo dále zpracovány.

Zákonné důvody zpracování

Podle směrnice o ochraně údajů mohou být osobní údaje zpracovány, pouze když toto zpracování vychází z jednoho z důvodů pro legitimní zpracování údajů²⁰.

Ve většině scénářů, kde se používá technologie RFID, bude jediným zákonným důvodem, jenž budou mít správci údajů k dispozici pro legitimní shromažďování informací prostřednictvím RFID, souhlas jednotlivých osob.

Je-li použit souhlas, podle směrnice o ochraně údajů musí splňovat tyto požadavky:

- Musí být udělen svobodně, to znamená, že musí být udělen bez „uvádění v omyl a bez nátlaku“.
- Musí být výslovný, jinými slovy, musí se týkat konkrétního účelu.
- Souhlas musí být vědomým projevem vůle.
- Souhlas musí být informovaný.

²⁰ Směrnice 95/46/ES článek (10)

- souhlas musí být „*nezpochybnitelný*“, což znamená, že souhlas, který může mít více než jeden význam, by se za souhlas nepovažoval.

Informační požadavky

Podle směrnice o ochraně údajů musejí správci údajů, kteří zpracovávají informace prostřednictvím technologie RFID, poskytnout subjektům údajů tyto informace:

- totožnost správce
- účely zpracování
- informace o příjemcích údajů a o existenci práva na přístup.

To znamená, že v souladu s touto povinností bude muset např. maloobchodní prodejna poskytnout subjektům údajů alespoň zřetelné oznámení o těchto skutečnostech:

- přítomnost štítků RFID na výrobcích nebo jejich obalech a přítomnost čteček;
- důsledky této přítomnosti v souvislosti se shromažďováním informací; správci údajů by měli zejména velmi zřetelně informovat, že přítomnost těchto zařízení umožňuje štítkům vysílat informace, aniž by se na tom dotyčná osoba musela aktivně podílet;
- účely, pro které mají být informace využity, včetně typu údajů, s nimiž budou informace RFID propojeny, a zda budou informace dostupné třetím stranám;
- totožnost správce.

Kromě toho v závislosti na konkrétním využití RFID bude správce údajů muset informovat také o tom:

- jak vyřadit z provozu, deaktivovat nebo odstranit štítky z výrobků a zabránit tak tomu, aby sdělovaly další informace,
- jak uplatňovat právo na přístup k informacím.

Zásada řádného zpracování uvedená v čl. 6 písm. a) směrnice o ochraně údajů vyžaduje, aby subjektu údajů byly informace poskytnuty zřetelně a srozumitelně.

A konečně, při poskytování výše uvedených informací považuje pracovní skupina za důležité zdůraznit, že by subjekt údajů měl být schopen pochopit důsledky použití RFID.

4.3 Doporučení pro provozovatele

Jedním z ukázkových využití RFID je v současné době pražská OpenCard. Tento projekt byl v mediích často komentovaný, neboť RFID systém použitý na OpenCard, by měl splňovat podmínky zákona na ochranu osobních údajů. Při hlubším zamyšlení však objevíme hned několik jeho nedostatků, které nejsou v souladu s bezpečným zpracováním. Pokud chce pražan využívat služeb OpenCard, musí předložit občanský průkaz – tímto krokem ztrácí její pořizovatel veškerou anonymitu a provozovatel služby získává informace o identitě uživatele a v závislosti na množství využívaných služeb i údaje o jeho soukromí. Pokud by totiž využíval služby, které OpenCard nabízí, tedy časová jízdenka pražské MHD, platba výpůjčného v knihovně, placení při využití parkování a přístup na web Magistrátu hlavního města Prahy, získá provozovatel ucelený pohled na náš život, pohyb po městě a mnoho dalšího, který bude kdykoliv přístupný oprávněným osobám. V případě tohoto velmi diskutovaného projektu byl vyvíjen tlak na bezpečnost zpracování pořízených dat a proběhla kontrola provedená Úřadem na ochranu osobních údajů se závěrem zlikvidovat již pořízenou databázi čipových karet a pouze kromě taxativně vymezených výjimek provozovat systém anonymně. Z provedených šetření byl vyvozen závěr, že uživatel má možnost rozhodnutí, zda chce používat kartu anonymní, nebo zda použije kartu s identifikátorem. U karet s identifikátorem musí provozovatel dodržovat určité povinnosti spojené s bezpečností zpracování poskytnutých údajů.

Z výše uvedeného příkladu je vidět, že ze strany provozovatelů RFID systémů by měla být vůle informovat potenciální i stávající zákazníky o tom jak

systém funguje, jak je manipulováno se shromážděnými daty a jak je zabráněno možnému zneužití nasbíraných dat.

Většina správců údajů opomíjí dodržování zákonem stanovených podmínek, především dodržování směrnice 95/46/EC, která určuje, že *„systémy zpracování údajů slouží lidem; (...) musejí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob, zejména právo na soukromí, a přispívat k hospodářskému a sociálnímu pokroku, k rozvoji obchodu, jakož i dobrých životních podmínek jednotlivců“*²¹ i přes skutečnost, že správci údajů mají povinnost přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení nebo neoprávněnému sdělování. Opatření mohou být organizační nebo technická.

Prioritou každého provozovatele systému RFID by měla v každém případě být povinnost dodržování zásad při shromažďování, zpracovávání a uchovávání svěřených dat v souladu s právními normami.

Zároveň už při návrhu aplikace ještě před jejím uvedením do provozu, by měly být aplikovány bezpečnostní prvky zabraňující zneužití shromažďovaných dat.

²¹ Směrnice 95/46/EC článek (2)

5. Dopady ochrany osobních údajů na uživatele

5.1 Možnosti ochrany osobních údajů

Právní normou pro ochranu osobních údajů je zákon č. 101/2000 Sb., o ochraně osobních údajů, kde jsou formulována práva a povinnosti provozovatelů, ale také jak se můžeme bránit. Asi nejjednodušší způsob ochrany je nedávat souhlas se zpracováním osobních údajů.

5.2 Práva při ochraně osobních údajů

Právní normou, která nám říká, jaká máme práva při ochraně osobních údajů je zákon č. 101/2000 S., o ochraně osobních údajů, kde se této otázce věnuje §21.

Podle tohoto paragrafu máme právo požadovat od správce nebo zpracovatele vysvětlení, nebo odstranění závadného stavu pokud je zpracování osobních údajů v rozporu s ochranou soukromého a osobního života, nebo v rozporu se zákonem, zejména jsou-li tyto údaje nepřesné s ohledem na účel jejich zpracování. Odstraněním závadného stavu se myslí zejména provedení oprav, doplnění nebo likvidace osobních údajů nebo blokace osobních údajů.

Správce nebo zpracovatel pokud je žádost opodstatněná, neprodleně odstraní závadný stav. Pokud by nám nechtěl správce nebo zpracovatel vyhovět, můžeme se obrátit na Úřad pro ochranu osobních údajů.

Pokud by nám vznikla jiná, než majetková újma budeme postupovat při jejím uplatňování podle §13 zákona č. 40/1964 Sb., občanského zákoníku.

Za porušení povinností při zpracování osobních údajů, odpovídají správce a zpracovatel společně a nerozdílně.

Umožnit subjektu údajů ověřit přesnost údajů a zajistit, že jsou údaje aktualizovány. Tato práva se v plném rozsahu použijí na shromažďování osobních údajů prostřednictvím technologie RFID.

Jestliže štítky RFID obsahují osobní informace popsané, měli by lidé mít nárok znát informace obsažené na štítku a opravovat je pomocí snadno dostupných prostředků.

5.3 Doporučení

V dnešní době se nelze vyhnout „špehování“. Skoro každý má internet, mobilní telefon, platební kartu a jejich používání je možné sledovat. Pokud chceme omezit možnost zcizení osobních údajů a sledování musíme si určit některé zásady.

Takové obecné zásady pro ochranu osobních údajů vydal i Úřad na ochranu osobních údajů na svých stránkách²². Jako jedna z důležitějších zásad je „pozorně si přečtěte dokument, který podepisujete.“²² Tato zásada neplatí jenom pro ochranu osobních údajů, ale kdykoliv po nás někdo chce něco podepsat. Další zásadou je, že „souhlas s poskytnutím osobních údajů musí být vědomý, svobodný a informovaný.“²²

Důležitá je také informovanost o nové technologii. Co nám může dát a co vzít. Mělo by nás zajímat jak technologie pracuje a jak nám zasáhne do života.

²² Zásady ochrany osobních údajů, Dostupné z URL:
<http://www.uoou.cz/uoou.aspx?menu=281&loc=454>

6. Závěr

Ochrana osobních údajů je jedno z témat, o kterém se neustále diskutuje. Existuje velké množství novinových článků, slyšíme o tomto tématu v televizi a s problematikou ochrany osobních údajů se setkáváme i v každodenním životě, aniž bychom o ní měli bližší povědomí.

Právě s problematikou ochrany osobních údajů se nás tato bakalářská práce snaží obeznámit. Nejprve jsme se seznámili se základními pojmy, například co slovní spojení osobní údaj znamená a kde je definováno. Dále jsme se zabývali zákonnou úpravou osobních údajů, a to jak z pohledu právních norem České republiky, tak i právních norem Evropské unie.

Každá moderní technologie, která se dotýká problematiky osobních údajů, má vždy dvě strany mince. Jednou z ní je technologický pokrok, který nás posunuje vpřed a usnadňuje nám práci. Druhou stranou je prolínání této technologie s naším soukromím, které může vyústit k osobním problémům. Výborným příkladem je právě RFID, ve kterém se zabýváme v jedné z částí bakalářské práce. RFID, jako takové, je u zrodu svého používání a je potřeba zvýšit povědomí o této technologii, s kterou se v budoucnu budeme setkávat mnohem více. Pokud bude tato technologie dobře aplikovaná, tak nám může pomoci například i v rámci boji proti terorismu.

Během průzkumů Evropské unie v roce 2006 o používání RFID čipů se ukázalo, že občané mají strach z narušení soukromí a zároveň potřebují a chtějí mít kontrolu nad informacemi, týkajícími se jejich osoby.

V závěru jsme si shrnuli dopady ochrany osobních údajů pro uživatele, možnosti ochrany a naše práva.

Použitá literatura:

- 1 Hradilová, Jitka. Ochrana osobních údajů v Evropské unii. Ikaros. Dostupné z URL <http://www.ikaros.cz/node/4552>
- 2 Jaké jsou přínosy a výhody RFID? RFID portál. Dostupné z URL http://www.rfidportal.cz/index.php?page=pouziti-prinosy_rfid
- 3 Listina základních práv a svobod. Dostupné z URL: <http://www.psp.cz/docs/laws/listina.html>
- 4 Zákon č. 1/1993 Sb., Ústava České republiky
- 5 Zákon č. 101/2000 Sb., o ochraně osobních údajů
- 6 Doporučení komise 2009/387/ES o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence. Dostupné z URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:CS:PDF>
- 7 Pracovní dokument o otázkách ochrany údajů, které souvisejí s technologií RFID. Dostupné z URL: http://www.uoou.cz/files/zahr_EK_WP29_105.pdf
- 8 Úřad pro ochranu osobních údajů Dostupné z URL: <http://www.uoou.cz/uoou.aspx>